Remarks

The above Amendments and these Remarks are in reply to the Final Office Action mailed January 30, 2007.

I. Summary of Examiner's Rejections

Prior to the Final Office Action mailed January 30, 2007, Claims 1-9 and 21-31 were pending in the Application. In the Office Action, Claims 1-9 and 21-31 were objected to because of informalities. Claims 1-2, 5, 7-8, and 21-31 were rejected under 35 U.S.C. 103(a) as being obvious over Johnson (U.S. Patent No. 6,295,607) in view of Brownlie et al. (U.S. Patent No. 6,202,157) and further in view of Donohue (U.S. Patent No. 6,199,204). Claim 6 was rejected under 35 U.S.C. 103(a) as being unpatentable over Johnson in view of Brownlie and Donohue and further in view of Wang (U.S. Patent No. 5,956,521). Claims 3-4 and 9 were rejected under 35 U.S.C. 103(a) as being unpatentable over Johnson in view of Brownlie in view of Donohue and further in view of TRCKA et al. (U.S. Publication No. 2001/0039579) and Microsoft Press (Computer Dictionary, 3rd Edition, ISBN:157231446XA, 1997).

II. Summary of Applicant's Amendment

The present Response amends Claims 1, 7, 21, 26 and 30-31, leaving for the Examiner's present consideration Claims 1-9 and 21-31. Reconsideration of the Application, as amended, is respectfully requested. Applicant respectfully reserves the right to prosecute any originally presented or canceled claims in a continuing or future application.

III. Claim Objections

In the Office Action mailed January 30, 2007, Claims 1-9 and 21-31 were objected to as containing informalities. More specifically, Claims 1, 21, 26 and 30-31 recited the term "the application" followed by "an application." The present Response hereby amends Claims 1, 21, 26 and 30-31 so as to provide proper antecedent basis for the terms therein. Applicant respectfully submits that as amended, Claims 1-9 and 21-31 no longer contain the above informalities and reconsideration thereof is respectfully requested.

IV. Claim Rejections under 35 U.S.C. § 103(a)

Claims 1-2, 5, 7-8, and 21-31 were rejected under 35 U.S.C. 103(a) as being obvious over Johnson (U.S. Patent No. 6,295,607, hereinafter Johnson) in view of Brownlie et al. (U.S. Patent No. 6,202,157, hereinafter Brownlie) and further in view of Donohue (U.S. Patent No.

6,199,204, hereinafter Donohue). Claim 6 was rejected under 35 U.S.C. 103(a) as being unpatentable over Johnson in view of Brownlie and Donohue and further in view of Wang (U.S. Patent No. 5,956,521). Claims 3-4 and 9 were rejected under 35 U.S.C. 103(a) as being unpatentable over Johnson in view of Brownlie in view of Donohue and further in view of TRCKA et al. (U.S. Publication No. 2001/0039579) and Microsoft Press (Computer Dictionary, 3rd Edition, ISBN:157231446XA, 1997).

Claim 1

Claim 1 has been amended to more clearly define the embodiment therein. As amended, Claim 1 defines:

> *1. A system for maintaining security in a distributed computing environment, comprising:*
>
> *(1) a policy manager, coupled to a network, including*
>
> *a database for storing a security policy including a plurality of rules that control user access to applications; and*
>
> *a policy distributor, coupled to the database, for distributing the plurality of rules through the network;*
>
> *(2) a security engine located on a client coupled to the network, for storing a set of the plurality of rules constituting a local customized security policy received through the network from the policy distributor, and for enforcing the local customized security policy with respect to an application at the client wherein enforcing the local customized security policy includes evaluating an access request by matching it to one or more of the plurality of rules of the local customized security policy and granting or denying access to the application based on the evaluation; and*
>
> *(3) the application, coupled to the security engine, wherein the security engine guards access to the particular application to which said security engine is coupled, such that each separate application in the system is guarded by a different security engine; and*
>
> *wherein the security policy is updated by recording a series of incremental changes to the security policy, determining which of said incremental changes are applicable to said security engine, computing an accumulated delta that reflects the series of incremental changes applicable to said security engine and sending the accumulated delta to the security engine from the policy manager such that the security engine uses the accumulated delta to update the local customized security policy.*

As amended, Claim 1 clearly defines an application that is coupled to a security engine such that the security engine guards access to the particular application to which it is coupled. In this way, each separate application in the system is guarded by a different security engine based on a centrally distributed security policy. Furthermore, Claim 1 has also been amended to more explicitly define that the security policy is updated by recording incremental changes to the security policy, determining which of those changes are applicable to each security engine and

then computing an accumulated delta that reflects only those incremental changes that are applicable to each different engine. At this point, the accumulated delta is distributed to the corresponding security engine so that it can be used to update the security policy.

Applicants respectfully submit that these features are not disclosed nor rendered obvious by Brownlie (U.S. Patent No. 6,202,157) in combination with Johnson (U.S. Patent No. 6,295,607) and further in combination with Donohue (U.S. Patent No. 6,199,204).

Firstly, the cited references fail to disclose a security engine coupled to the application wherein the security engine guards access to the particular application to which said security engine is coupled, such that each separate application in the system is guarded by a different security engine based on the security policy received from the policy distributor, as defined in Claim 1. For example, none of the cited references disclose a security engine that is coupled to an application. Furthermore, there is no disclosure whatsoever of each security engine guarding access to the particular application to which it is coupled, as defined in Claim 1. This feature of Claim 1 allows access to each separate application to be guarded by a different security engine based on a centrally distributed but locally customized security policy.

In the Office Action, Brownlie in combination with Johnson were cited as disclosing a security engine that controls access to applications. Applicant respectfully disagrees. The cited portions of Johnson describe an intermediary security server that contains security files for guarding access to applications and data that reside on an application server. These security files contain user Ids and passwords. The client thus appears to interact with the various applications but only through such a security server (SAS server) (Johnson, col. 5, lines 22-37, col. 5, line 65-col.6, line 5). As such, Johnson does not appear to be at all concerned with any security engine that is coupled to an application and that guards access to the application to which it is coupled. Instead, it merely uses an access control server as an intermediary between clients and the application server in order to enforce user IDs and passwords.

Similarly, Brownlie also fails to disclose any security engine that is coupled to an application and that guards access to the application to which it is coupled, as defined in Claim 1. Instead, Brownlie merely discloses that security policy data such as password length rules are distributed to the various network nodes for enforcement thereon. Thus, once a client has received a particular password lifetime policy, it will then restrict the user from continuing to use the password upon expiration of that lifetime policy. However, there is no disclosure in Brownlie of any security engine that is coupled to an application and that guards access to the particular application to which it is coupled. Further, there is no disclosure of each separate application in the system being guarded by a different security engine, as defined in Claim 1.

Secondly, Claim 1 has been amended to more clearly define the updating policy feature defined therein. As amended, Claim 1 defines that a series of incremental changes are first recorded and then it is determined which of those incremental changes are applicable to each security engine. From this, an accumulated delta is computed that reflects only those changes that are applicable to that specific engine. This delta can then be distributed to the corresponding engine.

In the Office Action, Donohue was cited as disclosing the updating feature of Claim 1. Applicant respectfully disagrees. Donohue teaches the distribution of software updates and patches. More specifically, Donohue provides an updater agent which is associated with a computer program and which accesses relevant network locations and downloads any available updates to that program (Donohue, Abstract). This is different from the features of Claim 1, as amended. For example, Donohue does not disclose any recording or keeping track of incremental changes to a security policy. More specifically, there is no disclosure of determining which of those incremental changes are relevant to each security engine and computing an accumulated delta that reflects only those changes that are applicable to each different security engine.

Furthermore, in the Office Action it was proposed that "updating by either use of a full update or incremental updates is simply an obvious variation of data update methodology well known in the art ... as commonly encountered in implementation of Microsoft patches, routing information synchronization and anti-virus software definition files updates." (Office Action, p. 3). Applicant respectfully disagrees. Even if it were known to distribute patches of a software program, there has been no disclosure whatsoever of recording incremental changes to a *security policy*. More importantly, none of the cited references disclose the specific technique used to update the security policy that is defined in Claim 1, as described above. It cannot be said that the specific updating methodology are merely an "obvious variation of possible security change implementations" (Office Action page 6) without providing any disclosure of such specific implementations. Donohue completely fails to mention any recording of incremental changes to a security policy and then determining which of those incremental changes are applicable to each different security engine. Furthermore, Donohue fails to disclose computing an accumulated delta that reflects only those applicable changes and distributing the delta to the corresponding security engine, as defined in Claim 1. Since Donohue fails to disclose any such implementation, it cannot anticipate nor render obvious these features of Claim 1.

Finally, in the Office Action it was proposed that:

> "in a network environment, it is infeasible to ensure that incremental changes are implemented by all subjects (clients with security engines) at the same time. For example, in addition to subjects available for updates, some may be shut down (e.g. user taking vacation), and some may not be even in a distributor network (e.g. user taking a laptop for a business trip). As a result, comprehensive updates to already present policy must account for the time difference that results in a different set of incremental changes distributed policy subjects. Thus, it would have been obvious to one of ordinary skill in the art ... to keep track of incremental changes that would allow computation of an accumulated delta..." (Office Action pp.6-7).

Applicant respectfully submits that the problems described by Examiner would not even exist prior to the system defined in Claim 1. In fact, the cited portion above reads on the various definitions of problems that are described in the present Application. There has been no disclosure in any of the cited references of such problems, nor solutions to any such problems as proposed in the Office Action. For example, none of the cited references appear to be at all concerned with the feasibility of ensuring that incremental security policy changes are implemented by all clients with security engines at the same time, as proposed in the Office Action. Accordingly, any such conclusion or interpretation would have to take into account techniques not known at the time of the invention and therefore must be drawn from impermissible hindsight.

In view of the above comments, Applicant respectfully submits that Claim 1, as amended, is neither anticipated by, nor obvious in view of the cited references, and reconsideration thereof is respectfully requested.

Claims 7, 21, 26, 30 and 31

Claims 7, 21, 26, 30 and 31, while independently patentable, recite limitations that, similarly to those described above with respect to Claim 1, are not taught, suggested nor otherwise rendered obvious by the cited references. Reconsideration thereof is respectfully requested.

Claims 2-6, 8-9, 22-25 and 27-29

Claims 2-6, 8-9, 22-25 and 27-29 are not addressed separately, but it is respectfully submitted that these claims are allowable as depending from an allowable independent claim, and further in view of the comments provided above. Applicant respectfully submits that Claims 2-6, 8-9, 22-25 and 27-29 are similarly neither anticipated by, nor obvious in view of the cited references, and reconsideration thereof is respectfully requested.

It is also submitted that these claims also add their own limitations which render them patentable in their own right. Applicant respectfully reserves the right to argue these limitations should it become necessary in the future.

V. Conclusion

In view of the above amendments and remarks, it is respectfully submitted that all of the claims now pending in the subject patent application should be allowable, and reconsideration thereof is respectfully requested. The Examiner is respectfully requested to telephone the undersigned if he can assist in any way in expediting issuance of a patent.

Enclosed is a PETITION FOR EXTENSION OF TIME UNDER 37 C.F.R. § 1.136 for extending the time to respond up to and including May 30, 2007. The Commissioner is authorized to charge any underpayment or credit any overpayment to Deposit Account No. 06-1325 for any matter in connection with this response, including any fee for extension of time, which may be required.

Respectfully submitted,

Date: May 30, 2007

By: /Justas Geringson/
Justas Geringson
Reg. No. 57,033

Customer No.: 23910
FLIESLER MEYER LLP
650 California Street, 14th Floor
San Francisco, California 94108
Telephone: (415) 362-3800
Fax: (415) 362-2928